AMENDMENT TO RULES COMMITTEE PRINT FOR H.R. 6395

OFFERED BY MS. ESHOO OF CALIFORNIA

Add at the end of subtitle C of title XVI the following:

SEC. 16___. IMPROVING CYBERSECURITY OF SMALL ORGANIZATIONS.

(a) DEFINITIONS.—In this section:

(1) ADMINISTRATION.—The term ''Administration'' means the Small Business Administration.

(2) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of the Administration.

(3) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(4) CYBERSECURITY BEST PRACTICES.—The term ''cybersecurity best practices'' means the cybersecurity best practices documented and promoted in the resource maintained under section 3(a).

(5) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

(6) NIST.—The term ''NIST'' means the National Institute of Standards and Technology.

(7) SECRETARY.—The term ''Secretary'' means the Secretary of Commerce.

(8) SMALL BUSINESS.—The term ''small business'' has the meaning given the term ''small business concern'' in section 3 of the Small Business Act (15 U.S.C. 632).

(9) SMALL BUSINESS DEVELOPMENT CENTER.—The term ''small business development center'' has the meaning given the term in section 3 of the Small Business Act (15 U.S.C. 632).

(10) SMALL BUSINESS LENDING COMPANY.—The term ''small business lending company'' has the meaning given the term in section 3 of the Small Business Act (15 U.S.C. 632).

(11) SMALL GOVERNMENTAL JURISDICTION.—The term ''small governmental jurisdiction'' has the meaning given the term in section 601 of title 5, United States Code.

(12) SMALL NONPROFIT.—The term ''small nonprofit'' has the meaning given the term ''small organization'' in section 601 of title 5, United States Code.

(13) SMALL ORGANIZATION.—The term ''small organization'' means an organization that is unlikely to employ a specialist in cybersecurity, including—

(A) a small business;

(B) a small nonprofit; and

(C) a small governmental jurisdiction.

(b) CYBERSECURITY BEST PRACTICES.—

(1) IN GENERAL.—The Director shall maintain a resource documenting and promoting cybersecurity best practices for use by small organizations, which shall—

(A) include simple, basic controls that have the most impact in protecting small organizations against common cybersecurity threats and risks;

(B) include best practices to address common cybersecurity threats and risks posed by electronic devices that are personal to the employees and contractors of small organizations, as well as electronic devices that are issued to those employees and contractors by small organizations; and

(C) recommend—

(i) types of commercial, off-the-shelf technology products and services that im-

prove the cybersecurity of small organizations; and

(ii) configurations and settings for some of the most commonly used software that can improve the cybersecurity of small organizations.

(2) CONSISTENCY.—The Director shall ensure the cybersecurity best practices are consistent with—

(A) cybersecurity resources developed by NIST, as required by the NIST Small Business Cybersecurity Act (Public Law 115–236); and

(B) the most recent version of the Cybersecurity Framework, or successor resource, maintained by NIST.

(3) UPDATES.—

(A) IN GENERAL.—The Director shall review the cybersecurity best practices not less frequently than annually and update them as appropriate.

(B) CONSULTATION.—In updating the cybersecurity best practices under subparagraph (A), the Director shall, to the degree practicable and as appropriate—

(i) consult relevant Federal and non-Federal experts; and

(ii) consult with small organizations, insurers, companies that work with small organizations, and academic and other experts in cybersecurity.

(4) USER INTERFACE.—As appropriate, the Director shall consult with experts regarding the design of a user interface for the cybersecurity best practices resource maintained under paragraph (1).

(c) PROMOTION OF CYBERSECURITY BEST PRACTICES FOR SMALL BUSINESSES.—

(1) PUBLIC AVAILABILITY.—The cybersecurity best practices resource maintained under subsection (b)(1) shall be—

(A) made available, prominently and free of charge, on the public website of the Cybersecurity Infrastructure Security Agency; and

(B) linked to from relevant portions of the websites of the Administration and the Minority Business Development Agency.

(2) PROMOTION GENERALLY.—The Director, the Administrator, and the Secretary shall, to the degree practicable, promote the cybersecurity best practices through relevant resources that are in-

tended for or known to be regularly used by small organizations, including in agency documents, websites, and events.

(3) PROMOTION AMONG RECIPIENTS OF SBA ASSISTANCE.—Not later than one year after the date of enactment of this Act, the Administrator shall—

(A) encourage the adoption of the cybersecurity best practices for small businesses that receive assistance from the Administration, including by requiring a brief description of how a small business will adopt the cybersecurity best practices or has instituted alternative practices or procedures that meet or exceed the intended outcomes of the cybersecurity best practices; and

(B) require entities that receive financial support from the Administration for the purposes of funding or supporting small businesses, including small business lending companies and small business development centers, to encourage adoption of the cybersecurity best practices.

(4) PROMOTION AMONG RECIPIENTS OF MBDA ASSISTANCE.—Not later than 180 days after the date of enactment of this Act, the Secretary shall encourage the adoption of the cybersecurity best

practices for small organizations that receive assistance from the Minority Business Development Agency, including by requiring a brief description of how a small organization will adopt the cybersecurity best practices or has instituted alternative practices or procedures that meet or exceed the intended outcomes of the cybersecurity best practices.

(5) RULE OF CONSTRUCTION.—Nothing in paragraphs (3) or (4) may be construed to require adoption of the cybersecurity best practices as a condition of receiving assistance from the Administration or the Minority Business Development Agency.

(d) REPORT ON INCENTIVIZING CYBERSECURITY FOR SMALL ORGANIZATIONS.—

(1) IN GENERAL.—Not later than six months after the date of enactment of this Act, the Administrator, in consultation with the Director and the Commission, shall submit to Congress a report recommending methods to incentivize small organizations to adopt products and services that promote the cybersecurity best practices, including cloud services.

(2) MATTERS TO BE INCLUDED.—The report required under paragraph (1) shall—

(A) identify barriers or challenges for small organizations in purchasing or acquiring products and services that promote the cybersecurity best practices, including cloud services;

(B) assess market availability, market pricing, and affordability of products and services that promote the cybersecurity best practices, including cloud services for small organizations, with particular attention to identifying high-risk and underserved sectors or regions;

(C) estimate the cost of tax breaks, grants, or other forms or subsidizing of products and services that promote the cybersecurity best practices, including cloud services, for small organizations; and

(D) as practicable, consult the certifications and requirement for cloud services described in the final report of the Cyberspace Solarium Commission established under section 1652 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 132 Stat. 2140).

(3) CONSULTATION.—In preparing the report required under paragraph (1), the Director shall consult with—

(A) the Secretary;

(B) the Administrator;

(C) the Commission; and

(D) small organizations, insurers, State governments, companies that work with small organizations, and academic and Federal and non-Federal other experts in cybersecurity.

(e) PERIODIC REPORT ON STATE OF CYBERSECURITY OF SMALL ORGANIZATIONS.—

(1) IN GENERAL.—Not later than six months after the date of enactment of this Act and not less frequently than annually for five years thereafter, the Administrator, in consultation with the Director, the Commission, and relevant Federal experts, shall submit to Congress and make publicly available a report on the state of cybersecurity of small organizations, including—

(A) adoption of the cybersecurity best practices among small organizations;

(B) the most significant cybersecurity vulnerabilities facing small organizations;

(C) the most common challenges facing small organizations in adopting the cybersecurity best practices;

(D) an estimate the economic cost of not accessing the products and services that promote cybersecurity best practices for small organizations; and

(E) as appropriate, policy recommendations for Congress to consider in legislation to enhance the state of cybersecurity of small organizations.

(2) FORM OF REPORT.—The report required under paragraph (1) shall be produced in unclassified form but may contain a classified annex.

☒